**YEARBOOK OF INTERNATIONAL & EUROPEAN CRIMINAL AND PROCEDURAL LAW**
Vol.2, 2023 Article 5

# Parallel Investigative Powers in the AFSJ's Criminal Procedural System

Christian Dukat

DOI:10.5281/zenodo.10684988

# Parallel Investigative Powers in the AFSJ's Criminal Procedural System

DOI:10.5281/zenodo.10684988

Christian Dukat, post Ph.D in European Criminal Law, UK

**Abstract**: Security, specialized agencies, crime prevention, and use of data are the elements that create a criminal and procedural security system today. Accelerate and try to interconnect the dangers that exist for safety and prevention we arrive at a preventive observation investigation. The network of the Justice and Home Affairs Agencies (JHA Network) and the “exchange of information” through data interoperability modifies the criminal procedural categories in the EU context. Information powers, authorities of an administrative nature and the future after the amendment of the EUROPOL with the Regulation 991 of 2022, as well as the proposal for a code of police cooperation in the territory of the EU is part of a fragmented system of criminal competition regarding the powers of prevention and investigation.

**Keywords**: AFSJ; European criminal law; European Union law; EUROPOL; JHA Network; European criminal procedural law; EPPO; Cybercriminality; ETIAS; EMPACT; Interoperability;

JHAN; anti money laundering; COSI; Law Enforcement Directive; Financial Intelligence Units; EPPO; Directive PNR; Regulation EES; Directive API; EURODAC; AESEA; EDPS; FRONTEX; EU-Lisa; SIS; Data Subjects Categorisation; Security Union Strategy; ERPIS.

## Introduction

The last decades in the European criminal law have entered some new notions to prevent, punish, investigate, control and observe crimes, attitudes, etc. We are talking about security (Henderson, 2005; Adler-Nissen, Gammetoft Hannsen, 2008), the creation of agencies (Cassese, 2012; Chamon, 2016; Wood, 2018) and the collection of data, especially of an electronic nature (Sicurella, Scalia, 2013; Floridi, 2018; Pagallo, Quattrocolo, 2018) within the Area of Freedom Security and Justice (AFSJ) with the ultimate goal of protection and in parallel of the power to report content of online service providers for a voluntary examination of their compatibility with their terms and conditions. It is introduced with the Regulation (EU) 991/2022, which in turn also seems to presuppose a proactive monitoring activity of EUROPOL[1].

[1]Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, PE/8/2022/REV/1, OJ L

An information system within a context that has actually highlighted the needs of private and public security as well as the security (Goldewijk, 2008) criminally relevant to the principle of territoriality from a procedural point of view and evidentiary by attributing an electronic trace[2], i.e. in external communication data and log files (de Capitani, 2020).

Electronic evidence and Big Data (Slobogin, 2018; Leiser, Custers, 2019)[3] are part of the related Regulation for production orders which allow the judicial authorities of a Member State to have direct access to these electronic evidence which are organized with this by all Member States of the Union (Mitsilegas, 2022)[4]. The proposals for a digitized security system have been going on for years now (Daska, 2018)[5] arriving at the authorization of 5 Apil 2022 of the Council of the Member States and at the second Protocol of Budapest on

169, 27.6.2022, p. 1-42.

[2] Better access to e-evidence to fight crime - Consilium (europa.eu)

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89-131.

[4] Proposal for a Regulation OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final-2018/0108 (COD). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final-2018/0107 (COD). https://db.eurocrim.org/db/en/doc/3646.pdf

[5] Permanent Representative Committee, n. 9296/22: https://data.consilium.europa.eu/doc/document/ST-9296-2022-INIT/en/pdf

cybercrime which has been adopted on 17 November 2021 by the Council of Europe. Already on 6 June 2019, the Council adopted the related mandate authorizing the European Commission to negotiate an agreement with the United States for access to electronic evidence and for greater judicial cooperation in criminal matters (Daskal, 2018)[6]. Investigation, speed with new techniques, tools to act and prevention and investigation activities are elements before the news of the crime arrived. As a monitoring for all infrastructures[7] that connects with the appropriate agencies and within AFSJ (Eckes, Konstatinides, 2011)[8]. Interoperability between banks are pieces of evidence for dataification of evidence towards a security transformation that allow agencies and the Union to categorize evidence and data.

[6]CLOUD Act (Clarifying Lawful Overseas Use of Data) of March 2018: https://www.justice.gov/criminal-oia/cloud-act-resources

[7]Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities COM/2020/829 final (16.12.2020). Directive for Security of Network and Information System (NSI2): https://digital-strategy.ec.europa.eu/en/policies/nis2-directive Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance), PE/41/2022/INIT, OJ L 333, 27.12.2022, p. 1–79.

[8]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), PE/86/2018/REV/1, OJ L 151, 7.6.2019, p. 15–69.

**Investigation, criminal justice cooperation, observation and EPPO**

The European Public Prosecutor's Office (EPPO) has paved the way for a coordination of investigations by putting into practice the Regulation 1939/2019 as a balance in the AFSJ. It is a change that calls state sovereignty and judicial policies into question both at the EU and at the national level for the future of control and coordination in this sector and above all the function of this type of office.

The EPPO stages and legitimizes the investigation at both the pre-investigative and subsequent levels as an elastic competence that expands in a way that neglects individual and personal guarantees. An office that collaborates within the spirit of the Title V, TFEU (Blanke, Mangiamelli, 2021) and EUROPOL[9], i.e. the initiator of this type of investigation formally outside the scope of national police work and OLAF[10] as well as the Financial Intelligence Unit[11] which have put a boundary between

[9] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (recast) (Text with EEA relevance), OJ L 138, 26.5.2016, p. 44–101. Commission Implementing Regulation (EU) 2016/974 of 17 June 2016 establishing the standard import values for determining the entry price of certain fruit and vegetables, OJ L 161, 18.6.2016, p. 25–26. Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, PE/8/2022/REV/1, OJ L 169, 27.6.2022, p. 1–42.

[10] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, op. cit.

[11] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8

investigation and monitoring of observations at a European level.

The observational monitoring powers are embraced with that criminal investigation that often gets confused with the European political-institutional balances. Some agencies working alone in the space of AFSJ and the European Travel Information and Authorization System (ETIAS) (interoperability system) with various banks (such as EUROPOL) in order to power filters of collaboration with private entities to obtain electronic information contributing thus to the preservation production of this type of evidence.

## JHA Network and data and information exchange in the AFSJ

There are now many agencies at the European level and some of them are not connected to an AFSJ where they allow not only access to the lists of databases but also in an interconnected way power to the European digital interoperability[12]. The Justice and Home Affairs Agencies Network" (JHAN)[13] which dates back to

June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, op. cit., par. 4 and 7.

[12]Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (Text with EEA relevance), PE/87/2021/REV/1, OJ L 150, 1.6.2022, p. 1–19.

[13]See the relevant report: Report on JHA Network Activities 2021 - eucrim

2010 within the scope of the Council[14] as one of the agencies of the AFSJ shows a scope of justice and home affairs which dates back as early as the Treaty of Maastricht which presents itself as less regulatory and with more operational powers. Operational activity is strongly interlinked with the national law enforcement communities (Luchtman, Vervaele, 2014).

Cooperation bodies of the Union are interested in the common interest of the administration of justice and to internal affairs. Already since 2012, about nine agencies are part of the network, i.e. EUROPOL, EUROJUST, the External Action Service (EEAS or FRONTEX), which includes EU SITCEN, the European Agency for large-scale IT systems (eu-LISA), the Fundamental Rights Agency (FRA), the European Police College (CEPOL), the European Asylum Support Office (EASO), the European Institute for Gender Equality (EIGE), the European Monitoring Center for Drugs and Drug Addiction (EMCCDA), etc.

Within this whole maze of agencies, networks, which collaborate with each other or not, we notice models of collaboration that arise from the conclusion of bilateral, trilateral contacts and in an extended way through (since 2018 in the European Asylum Support Office (EASO), FRONTEX and

[14]Standing Committee on Operational Cooperation on Internal Security (COSI): https://eur-lex.europa.eu/EN/legal-content/glossary/standing-committee-on-internal-security.html

EUROPOL) cooperation of information on movements of a secondary type within the European ambit and in the other countries of the Schengen area with the aim of international protection, irregular immigration and the smuggling of migrants (from 2019 and on)[15]. Such a collaboration is based on guidelines concerning above all problems of the Afghan citizens.

Following a proposal from EUROPOL, the Standing Committee on Operational Cooperation on Internal Security (COSI) formed an ad hoc reference group, i.e. the hub team which operates from 2020 and constitutes contact points between all agencies in the JHA network which are united in the Home Affairs Directorate and at the Joint Research Center of the European Commission and the Counter-Terrorism Coordination Office.

**Are EMPACT and JHA Network a new type of EUROPOL?**

The European Multidisciplinary Platform Against Criminal Threats-EMPACT which collaborates with the JHA Network is actually a new EUROPOL which plans on a four-year basis an operational approach integrating internal security[16], the tools of external police border controls, the management and the

[15]European Monitoring Centre for Drugs and Drug Addiction (EMCDDA): https://www.emcdda.europa.eu/index_en

[16]https://www.consilium.europa.eu/media/53982/2021_645_002_empact-joint-communication-strategy_11-hor_web-acces.pdf

exchange of information, to prevention[17], at the "external border" of an internal security of the Union through public-private partnerships. A partnership of a political type dating back to 2012-2013 and operating within a circular system which between 2014 and 2017 as well as between 2018 and 2021 provided for graduation steps by identifying the new threats that had existed for years in the European context. The Council of the Europe has pre-established some priority areas for EMPACT 2022-2025 which have the internal security of the Union as their ultimate goal. We are referring to the EU Serious and Organized Crime Threat Assessment (EU SOCTA) which was created by EUROPOL on a form where the Council of the EU defined its priorities as serious and organized crime and as a key role in EMPACT. The identification of a limited number of such priorities operate through the Council as a multi-year master plan with strategic objectives of a horizontal nature involving the use of preventive and repressive measures. One more step prepared by the Standing Committee on Operational Cooperation on Internal Security (COSI) which it adopts every year independently and effectively the entire plan.

We are talking about a New Security Union Strategy that was presented by the Commission in July 2020[18] as a type of

[17]Terms of Reference as a key of EMPACT: "(…) (T)the intelligence-led approach based on a future-oriented and targeted approach to crime control, focusing upon the identification, analysis and "management" of persistent and developing "problems" or "risks" of crime" (…)".

[18]European Union New Security Union Strategy connecting the dots in a new

fundamental action that adopts and tackles organized crime, including human trafficking. Two strategies, i.e. the EU Strategy to Tackle Organized Crime 2021-2025 and the EU Strategy on Combating Trafficking in Human Beings 2021-2025, have been referred to SOCTA highlighting the illicit activities which are brought about by the Covid-19[19] outbreak. A strategy that refers to legislative proposals where the European Commission has the possibility of adopting an act of secondary law to form the EMPACT as a lively tool for operational cooperation, prevention and fight against organized crime.

**Probative value of a multifunctional nature and crime prevention**

Continuing forms of cooperation and collaboration for criminal prosecution show trends that concern the boundary between evidentiary elements, data that risk accompanying and distinguishing the concepts of evidential use and, possibilities

security ecosystem:
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[19]See: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy, COM/2020/605 final. Fighting organised crime-EU strategy for 2021-25: Fighting organised crime – EU strategy for 2021-25 (europa.eu). European Union serious and organised crime threat assessment (EU SOCTA 2021): European Union Serious and Organised Crime Threat Assessment 2017 | Europol (europa.eu) . COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy to tackle Organised Crime 2021-2025, COM/2021/170 final.

that express and provoke doubts for the applicable rules of the data itself.

Within this spirit we note the Regulation 679/2016-GDPR (Liakopoulos, 2019)[20] as a basis of information activity, for the prevention, investigation and prosecution of crimes, as well as of criminal execution based on Directive 680/2016/EU, Law Enforcement Directive (LED) (Brewczyńska, 2022)[21].

Already with the Framework Directive 2002/58/EC on personal data and the protection of privacy from electronic communications[22] the CJEU has taken an interpretative position by replacing the related Regulation on privacy and electronic communications as the subject of legislative negotiations. Functions of an administrative nature, prevention and penal repression generate many doubts about disciplines that are applicable such as for example to Financial Intelligence Units (FIU), as a trend of a category that arises from a continuous and progressive function in data regulation to a function which

[20]Proposal for a Regulation OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final.

[21]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

[22]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

concerns the conservation of materials, elements of evidence of a multifunctional nature and with objectives:

"(...) 1) that of preventive observation, arriving in hypotheses to coagulate a crime report; 2) subsequent to that of the continuation of the criminal investigation or the precautionary action; in cases where there are no explicit bans on usability; 3) to the decisions on the criminal judge. In short, in fact and almost inadvertently, the "data" pre-exists the criminal proceeding (provided it does not represent information in transit, otherwise it would fall within the concept of interception), ends up being pigeonholed in our traditional taxonomy of criminal proceedings, within the category of evidence documentary (…) trait d'union represented by the interoperability of the databases (legally envisaged)[23]. It is evident that the problem risks

[23]See in particular: Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification), OJ L 77, 23.3.2016, p. 1–52. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, PE/30/2019/REV/1, OJ L 135, 22.5.2019, p. 27–84. Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, PE/88/2018/REV/1, OJ L 135, 22.5.2019, p. 1–26. Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, PE/31/2019/REV/1, OJ L 135, 22.5.2019, p. 85–135. Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, PE/29/2018/REV/1, OJ L 295, 21.11.2018, p. 99–137. Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, PE/35/2018/REV/1, OJ L 312, 7.12.2018, p. 14–55. Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No

amplifying itself, since the activity of massive data collection (…) leads to the preconstitution of equally massive quantities of these amphibious elements (…) a criminal procedure outside the criminal procedure (…)"[24].

The data as an element of proof becomes a precise reality which also demonstrates the basis for preliminary rulings as can be seen from the jurisprudence of the CJEU in the discretion of national law which determines the conditions, the authorities and the providers of electronic communications services which exploit the data in your possession. A framework of stability between national rules which are thus presented with a third party and impartial controller so that the personal data are objects which attack, i.e. have sufficient guarantees against the risks of abuse[25]. A legislation of a national nature which seeks to regulate the authorities, traffic and location data[26] by limiting

1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, PE/36/2018/REV/1, OJ L 312, 7.12.2018, p. 56–106. Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, PE/21/2018/REV/1, OJ L 236, 19.9.2018, p. 1–71. Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327, 9.12.2017, p. 20–82.

[24]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), op. cit.

[25]CJEU, C-746/18, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) of 2 March 2021, ECLI:EU:C:2021152: not yet published, par. 41.

[26]Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive

access to authorities which respond to the purposes which pursue this kind of legislation and which provide for substantive and procedural conditions which regulate this type of use.

This kind of tendency for the use and collection of data as evidence is also seen in the reform of EUROPOL as noted in art. 2, lit. p) and q)

"(...) between administrative personal and investigative data: the former are those "processed by Europol and are different from operational personal data", and the latter are those that "a Member State, the European Public Prosecutor ("EPPO") (…)",

Eurojust or a third country is authorized to deal in the context of an ongoing criminal investigation, related to one or more Member States, in accordance with the applicable procedural rules and guarantees under EU or national law, or that a Member State, the EPPO, Eurojust or a third country has provided Europol with support in the ongoing criminal investigation, containing personal data which do not concern the categories of data subjects[27]. This type of coordination of the activities of the databases runs the risk of not following the chosen path, i.e. the investigative one, and following other purposes that come out of the European criminal and procedural law context.

2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, p. 11–36.

[27]Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, op. cit.

**Exchange of information: European Travel Information and Authorization System (ETIAS) and safety protection**

The European Travel Information and Authorization System (ETIAS)[28] is an information and authorization system in the travel sector[29] dealing with individuals who want to enter EU countries and who do not already use a visa[30]. European border management needs accurate information about travelers entering the territory of the EU, i.e. a valid recognition given by the ETIAS. The ETIAS[31] is part of a system of powers of both criminal and administrative nature latu sensu in the midst of interoperability between databases which are based on the relevant Regulation. The ETIA Regulation forms a protection within the borders of the EU which creates a unitary and complete legal framework as already noted by the EES

[28]Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, PE/21/2018/REV/1, OJ L 236, 19.9.2018, p. 1–71.

[29]ESTA (Electronic System for Travel Authorization: www.esta.cbp.dhs.gov/ and the eTA Program (Electronic Travel Autorisation): www.canada.ca/en/immigration-refugees-citizenship/services/visit-canada/eta.html

[30]See, Recital no. 40 of the ETIAS Regulation, in fact states: "(A) for the purpose of combating terrorist offenses and other serious crimes and taking into account the globalization of criminal networks, it is essential that the designated authorities competent for the prevention, detection and investigation of terrorist offenses and other serious crimes ("designated authorities") have the information they need to effectively carry out their duties. Accessing data contained in the VIS for such purposes has already proven effective in helping investigators make substantial progress in cases relating to trafficking in human beings, terrorism or drug trafficking. The VIS does not contain data on visa-exempt third-country nationals" (emphasis ours). Consider that there are currently 60 countries whose citizens do not need a visa to enter the European Union.

[31]https://travel-europe.europa.eu/etias_en

Regulation[32] and the PNR Directive[33] having as objectives the protection and prevention of criminal prosecution investigation for terrorism offenses and serious crimes such as for example the API Directive[34] under modification. The ETIAS works to pre-assess visa-free access to the Schengen area by allowing Member States to deny authorization for travelers to pre-screening which is carried out to avoid security threat, risk from irregular migration and public health, i.e. principles of European limitation which are part of the history of the Union as well as the related jurisprudence.

ETIAS guarantees a system of interoperability with others of an information nature such as for example SIS II and the Entry-Exit

[32]Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, p. 60–81. Commission Regulation (EU) No 1067/2011 of 18 October 2011 establishing a prohibition of fishing for horse mackerel and associated by-catches in EU waters of IIa, IVa; VI, VIIa-c, VIIe-k, VIIIa, VIIIb, VIIId and VIIIe; EU and international waters of Vb; international waters of XII and XIV by vessels flying the flag of Spain, OJ L 277, 22.10.2011, p. 9–10. Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327, 9.12.2017, p. 20–82.

[33]Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

[34]Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, p. 24–27.

System (EES)[35], VIS[36], EURODAC, EUROPOL and INTERPOL databases where this interoperability is not only part of art. 11 of the ETIAS Regulation but also of the second paragraph which provides for the amendments for regulatory acts enabling the information systems of the EU which are necessary to establish interoperability with the ETIAS and the provisions of the Regulation as the subject of a separate legal act. The Regulation and operation of ETIAS focuses on a European system such as the Common Identity Repository, i.e. of a multiple identity covering both databases, areas of police and judicial cooperation in criminal matters as well as areas of asylum and immigration in legal and political processing.

Threat risk is certainly always high and varied as a definition reaching an unlimited degree of abstraction.

[35] EUR-Lex - 4374366 - EN - EUR-Lex (europa.eu)

[36] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180, 29.6.2013, p. 1–30.

**(Follows): The Financial Intelligence Units and Anti-Money Laundering and Financing of Terrorism. What security systems do we have?**

Observational preventive monitoring launches itself into a sphere of control which envisages money laundering (Gilmore, 2004; Bergström, 2011) and the financing of terrorism which is built around a concept such as that of a suspicious operation with transfers of exchanges of communications beyond related data. The National Central Units (Financial Intelligence Units, FIUs) have entered this circle with the analysis objectives of reporting suspicious transactions[37], as well as information having to do with money laundering, illegal terrorism financing and, crimes connected with this type of activities. Already the reform of EUROPOL with art. 4, paragraph 1, lett. z) provided for the exchange of information and direct collaboration through contact with the FIUs.

The margin of appreciation that is provided to the national legislator, as well as the possibility of configuring the FIU as an administrative authority (a specialized structure for the police force) is a structure that enters the ambit of the judicial authority in countries that also adopt mixed solutions. According to paragraph 4 of the aforementioned provision: carry out the analysis of the financial flows on suspicious transactions (letters

[37]Committee of Experts on the Evaluation of anti-Money Laundering and Financing of Terrorism-MONEYVAL: https://www.coe.int/en/web/moneyval

a) and b)); it can suspend, for a maximum of five working days, operations that are always suspicious, even at the request of another intelligence unit, where this does not prejudice the course of the investigation (letter c); can carry out checks, “also through inspections”, in order to ascertain compliance with the provisions on the prevention and combating of money laundering and terrorist financing, with regard to reports of suspicious transactions and cases of omitted reporting of suspicious transactions, as well as with regard to the communications envisaged by the same decree and in cases of omission of the same, also with the assistance of the special currency police unit (letter f); it can then ascertain and contest or transmit to the supervisory authorities of the sector, the violations of the obligations of the aforementioned decree of which it becomes aware during the exercise of its institutional functions. The “unit” then ensures information to the national anti-mafia and anti-terrorism directorate (pursuant to article 6, paragraph 5, anti-money laundering decree); moreover, to carry out all the functions and tasks assigned to it by art. 6, paragraphs 4 and 5 of the aforementioned decree, it is guaranteed access to the tax register, the real estate register and the appropriate sections of the register of companies. Then there are real osmoses between the “administrative” activity of the same “Unit” and the activities of other public administrations, self-

regulatory bodies, i.e. the "competent authorities". This exchange concerns information for the prevention, detection and fight against money laundering and associated predicate offenses or the analysis of information relating to terrorism or organized crime associated with terrorism[38].

It is a type of treatment that defines and effects many contrasts as we see in theory and in practice over the next few years.

**Civil Aviation Safety (ANSV), European Aviation Safety Agency (EASA)**

When we talk about safety in the civil aviation sector, as well as about aviation safety, we talk about safety and security through a system of sources that dates back to Regulation 996/2010[39] and later with Regulation 1139/2018 with the implementing regulations also in various national offices[40].

[38]Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), op. cit.

[39]Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC Text with EEA relevance, OJ L 295, 12.11.2010, p. 35-50.

[40]Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and

The Regulation 996/2010 provides for the autonomous and incisive powers of the national agencies of reference (investigative authorities for civil aviation safety). Articles 1 and 5 clarify that the object of the Regulation is the improvement of safety in the aviation sector and the guarantee of a high level of efficiency, timeliness and quality of European civil aviation safety investigations, also specifying as the "sole objective" the prevention of future accidents and incidents and not the attribution of blame or liability[41].

This is both a punitive and a preventive profile where the Regulation focuses on the principles of autonomy, functional independence and investigative authority for civil security according to art. 5 which respects the aeronautical authorities. Any party or body whose interests or purposes may conflict with the task assigned to it or influence its objectivity (art. 4, paragraph 2) it is prescribed that said authority cannot solicit or receive instructions from any external subject and enjoys "unlimited authority over the conduct of safety investigations" (Article 4, paragraph 3), and the tasks entrusted to the investigative authority[42].

2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance), PE/2/2018/REV/1.

[41]Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC, Text with EEA relevance, OJ L 295, 12.11.2010, p. 35-50.

[42]Regulation (EU) No 996/2010 of the European Parliament and of the Council of

We continue with articles 8, 9, 10, 40 and 41 which are part of the anti-money laundering system as envisaged by the Unit to an investigative anti-mafia system suitable for legal proceedings in progress to information necessary for the identification of possible correlations between product flows at risk and suspicious financial flows, receiving from the National Directorate (except for investigative confidentiality), the confirmation of the usefulness of such information. However, the methods and times of transmission are left to the Protocols stipulated between the communicating authorities. Close informational and operational collaboration is then provided for by art. 9. Suspicious reports issued by the Unit, pursuant to art. 40 "even with the powers attributed to the Corps by the currency legislation", says article 9, paragraph 4, letter a)[43].

The applicability of GDPR, LED and FIU, as well as the national system reinvigorate the anti-money laundering and anti-terrorism (AML/CTF) system. In particular, the FIU created and built on the 5th Anti-Money Laundering Directive for the internal market. Article 41 of the directive applies to GDPR and is refering to the subjects obliged to transfer information concerning the related transactions of a suspicious nature. There is no clarity regarding Art. 18 of the Directive 2019/1153 which

20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC, op. cit.

[43]Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC, op. cit.

allows to protect the rights of the interested parties which are limited according to the GDPR, as well as LED does not explain how the FIU processes personal data in the performance of its tasks. The applicability of the LED according to Articles 8, 9 and the Directive 2019/1153[44] are part of a safety system that extends to the collection and analysis of information relating to aviation safety, for the purpose of preventing accidents, in activities that compromise one's independence and responsibilities of a regulatory, normative and administrative nature.

The questions are many in relation to the competition of the powers belonging to the judicial authorities. Doubts as to the mandatory nature of an initiative which is provided for by European sources (Article 5, paragraph 1) fall within the discretion of the independent authorities. Paragraph 5 of the provision states that:

"(...) investigations are conducted independently and separately from any judicial or administrative proceedings aimed at ascertaining guilt or liability", and they must not however cause prejudice to such proceedings. According to Article 12 of the Regulation the independence of the Safety Investigation Authority must allow for the technical investigation to be conducted with diligence and efficiency. They (the authorities) must take into consideration (at least) the strategic, and more sensitive, issues in the interaction between the administrative and judicial investigation, namely: access to the scene of the accident; storage of evidence and access to it; initial and transaction reports; information exchanges; the appropriate use of security information

[44]Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, PE/64/2019/REV/1, OJ L 186, 11.7.2019, p. 122–137.

and; lastly, regulating the methods of resolving any conflicts in the context of the balance and distribution of powers in the multilevel. Then the Member States must communicate these agreements to the Commission which, in turn, will have to communicate them to the president of the network of flight safety authorities, to the European Parliament and to the Council, in order to ensure adequate "information". If the agreement in the individual case is not reached on the basis of these agreements within a reasonable period, and not exceeding two weeks following the request, the investigator of the safety authority is not prevented from carrying out the examination or analysis anyway. However, where the judicial authority has the right to seize any evidence, the investigator will have immediate and unrestricted access to this evidence and will be able to use it"[45].

A fine balance largely depends on loyal cooperation through the judiciary and administrative authority. The Regulation 996/2010 and the national authority for flight safety (ANSV) has tried to avoid overlaps of a harmful nature as since 2014 has stipulated collaboration agreements with national magistrates to regulate flight safety. Already Article 9 of the Regulation 996/2010 states that:

"(...) any person involved who is aware of an accident or a serious incident must immediately communicate this information to the competent investigation authority for safety (...)"[46].

Regulation 1139/2018 also spoke of a:

"(...) high and uniform level of civil aviation safety through the adoption of common safety standards and through measures aimed at ensuring the conformity of each product, and the observance of every person and organization involved in civil aviation activities in the Union with regard to those common standards (…)"[47].

[45]Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, PE/64/2019/REV/1, op. cit.

[46]Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC, op. cit.

[47]Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC)

The same Regulation also created the European Aviation Safety Agency, the National Civil Aviation Authorities and, the European Commission and the European Aviation Safety Agency (EASA)[48]. The AESEA is in charge of regulating the legislative acts with the European Commission. According to Art. 83 of Regulation 1139/2018, the Agency has investigative powers, which are instrumental to the performance of the tasks related to certification and surveillance, specified in Article 62, paragraph 2. It performs, on its own behalf or through the competent national authorities or qualified subjects, "the necessary investigations". Also in this case we are dealing with investigations carried out in an "administrative" context, nevertheless the methods and results of the same are not insignificant for this reason. It is authorized to carry out even incisive activities, such as asking the natural or legal persons to whom it has issued a certificate, or who have made it a declaration, to provide the Agency with all the necessary information, and oral explanations regarding any fact, document, object, procedure or other matter relevant to

No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.

[48]Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.

determining whether the person complies with this Regulation and with the delegated and implementing acts adopted on the basis thereof, access the premises, land and means of transport "relevant" of such persons; as well as examining any relevant documents, records or data held by (or accessible to) such persons, as well as extracting copies or taking excerpts, regardless of the medium on which the information is stored[49].

In order to determine whether a person has issued a certificate and/or made a declaration in accordance with the spirit and content of the Regulation, the Agency is competent to make the relevant inquiries to any natural or legal person who may have information which is pertinent and which may log into.

Within this type of right/power, general protection clauses are also noted where they must respect the national law of the Member State or third country in which the investigation takes place, taking into account the rights and legitimate interests of the persons concerned and in compliance with the principle of proportionality[50].

[49]Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.

[50]Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament

According to Article 82, paragraph 2 of the Regulation 1139/2018

"(...) to access the relevant premises, land and means of transport referred to in letter c) a prior authorization from the judicial authority is required, in accordance with the applicable national law or administrative authority of the Member State or third country in question"[51].

These powers are exercised only once prior authorization has been obtained. The Agency shall ensure that its staff members and, where appropriate, other experts involved in the investigation are sufficiently qualified, receive appropriate instruction and are duly authorised, and that they exercise their powers upon presentation of written authorisation. Officials of the competent authorities of the Member State in whose territory an investigation is to be conducted assist in carrying out the activities at the request of the Agency, which must inform the Member State concerned in good time before the investigation.

**EUROPOL after the Regulation 991 of 2022**

Already in the Regulation of EUROPOL, the methods of exchange of information reinvigorate the role of data protection management, as well as the creation of a new supervisory body which provides for the right of access to personal data, the opposition mechanisms and the possible management illegitimacy of the data itself.

and of the Council and Council Regulation (EEC) No 3922/91.

[51]Artt. 2, 3, 4.

Regulatory innovations such as a construction site in the interior of the EU are driven by a dangerous transactionality of the use of data, i.e. as evidence leading to the network[52]. Innovations that behave like a collaboration between national and European authorities and between Agencies of the Union that interconnect with the search for available data and the usefulness of information between private operators by Internet Service Providers.

The Regulation EUROPOL 2017 has operational intersections such as FRONTEX, EU-LISA, SIS and ETIAS. The Regulation (EU) 991/2022, approved on 8 June 2022 seeks to reinvigorate the related interventions. The reform also tends to resolve the interinstitutional tension between EUROPOL and the European Data Protection Supervisor (EDPS). Already on 21 December 2021 EDPS signed a decision against EUROPOL based on Article 18, par. 5 of the current Regulation trying to cancel within six months of receiving the relevant decision the data it has in its hands and which have not been subjected to the Data Subjects Categorization (DSC) (Quintel, 2022).

The DSC identifies data, suspected individuals, contacts and possible victims as well as witnesses and information sources

[52]Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, PE/8/2022/REV/1, OJ L 169, 27.6.2022, p. 1–42.

(Nunzi, 2007) that are related to criminal activity. Thus EUROPOL noted that:

"(…) EDPS Decision will impact Europol's ability to analyse complex and large datasets at the request of EU law enforcement".

This concerns data owned by EU Member States and operational partners and provided to Europol in connection with investigations supported within its mandate. Frequently entails a period longer than six months, as do the police investigations it supports. It will seek the guidance of its Management Board and will assess the EDPS Decision and its potential consequences for the Agency's remit, for ongoing investigations as well as the possible negative impact on the security for EU citizens[53].

The key points allow EUROPOL to perform an operation through the processing of complex personal data bases and the relative classification of the interested parties as: Data Subject Categorization (DSC), according to the objectives of law enforcement.

EUROPOL is able to use related data that have no relation with subjects that have to do with the investigation[54]. The Regulation

[53]Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, op. cit.

[54]Art. 18 provides, in paragraph 1, that "(i)nsofar as it is necessary to achieve the objectives set out in Article 3, Europol may process information, including personal data". In paragraph 2, then, it provides that "(i) personal data may be processed only for the purposes of: a) cross-checks aimed at identifying links or other pertinent nexuses between information concerning: i) persons suspected of having committed a crime falling within the competence of Europol or have participated in it, or have been convicted of such an offence; (ii) persons in respect of whom there are concrete indications or reasonable grounds to believe that they may commit criminal offenses

allows the Agency the ability to carry out a retroactive analysis to enhance the effectiveness of data processing without DSC and thus to expand the information, conditions, possibilities of protecting the data collected during the past years and over time requires an aid to an investigation, such as a transitional regime dealt with by EUROPOL and even before the amendments of the Regulation.

Collaboration with private individuals on electronic evidence to receive data that is relevant to the investigation are norms of a

falling within the competence of Europol; b) strategic or thematic analyses; c) operational analyses; d) facilitation of the exchange of information between Member States, Europol, other Union bodies, third countries, international organizations and private parties; e) innovation and research projects; (f) support to Member States, upon their request, in informing the public about suspected or convicted persons who are wanted on the basis of a national judicial decision relating to a criminal offense falling within the scope of Europol's objectives, and facilitation of communication of information about these persons, to the Member States and to Europol by citizens. The discipline can only be understood by reading Annex II to the Regulation. It makes a distinction (indicated with the letters "A" and "B", between the Categories of personal data and categories of data subjects for the purposes of the cross-checks referred to in Article 18, paragraph 2, letter a); and the categories of personal data and of interested parties for the purposes of strategic or thematic analyses, operational analyzes or facilitation of the exchange of information, referred to in Article 18, paragraph 2, letters b), c) and d). Letter "A" not only concerns persons who, under the national law of the Member State concerned, are suspected of having committed or taken part in a crime falling within Europol's jurisdiction, or who have been convicted of such a crime, but also persons in respect of whom there are concrete indications or reasonable grounds, under the national law of the Member State concerned, to believe that they may commit criminal offenses falling within the competence of Europol. Instead, the persons referred to in letter "B" are those who, under the national law of the Member State concerned, are suspected of having committed or taken part in a crime falling within Europol's competence, or who have been convicted for such an offence; (b) persons in respect of whom there are concrete indications or reasonable grounds, under the national law of the Member State concerned, to believe that they may commit criminal offenses falling within the competence of Europol; c) persons who may be called upon to testify in the course of investigations into the offenses involved or subsequent criminal proceedings; d) persons who have been victims of one of the crimes in question or for whom certain facts lead to the conclusion that they could be victims of such an offence; e) contact and support persons; and f) persons who can provide information on the crimes in question (...)".

specific nature for cooperation in times of crisis and when dealing with child sexual abuse. In online crisis situations, we note the dissemination of content relating to an ongoing or recent event in the real world which portrays damage to life or physical integrity or which refers to imminent damage to life or physical integrity and which have the objective or effect of seriously intimidating the population, provided that there is a link or a reasonable suspicion of a link to terrorism or violent extremism and that the exponential multiplication and virality of such content between various online services is expected (Mitsilegas, Mouzakiti, 2020).

The Regulation has sought to reinvigorate the protection of individuals[55] as well as the control of the European Parliament and the accountability of the Agency[56]. These are innovations that are connected with EUROPOL asking the authorities of each Member State for a cross-border dimension of the crime in specific cases which embraces criminal investigation in a positive way, thus coordinating and influencing the common interest of the Union. Reinvigorating cooperation internally, and with the EPPO externally, concerns profiles that are oriented

[55]Fundamental Right Officer (FRO): https://frontex.europa.eu/careers/who-we-are/structure/specific-functions/fundamental-rights-office/

[56]European Data Protection Supervisor (EDPS): https://edps.europa.eu/_en. European Economic and Social Committee (EESC): www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/strengthening-europols-mandate. EDPS Opinion on the Proposal for Amendment of the Europol Regulation: www.edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf.

towards collaborations with third countries for anti-terrorism objectives and collaboration with private individuals by obtaining e-evidence.

The reform of the EUROPOL goes hand in hand with this of the Regulation of the Schengen Information System (SIS)[57] where EUROPOL inserts into the SIS system data that individuals from third countries are involved in an innovation activity that overcomes the bottleneck of the regulatory package within a production of continuous electronic evidence in the European context and beyond.

[57]Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, PE/36/2018/REV/1, OJ L 312, 7.12.2018, p. 56–106.

## Concluding Remarks

Observational monitoring is formed through a prevention and an investigation plan and by the penal repression of the EU. It is still a step forward, towards protection and security in the AFSJ through bilateral, trilateral and multilateral agreements which however produce a fragmentation that could become perhaps not so functional in the near future[58].

Within the family of the Security Union Strategy, the European Commission has already decided since April 2021 to carry out a consultation of a public nature that has to do with the modernisation, improvement and reinvigoration of cross-border cooperation.

Already the European Commission from 8 December 2021 through the proposal for a Recommendation for the Council on operational police cooperation has tried to give greater protection to police operators in all the countries of the European Union which are related and named as "cross-border hot pursuits, surveillance, joint patrols and other joint operations" such as a proposal for a Regulation based on automated data exchange for related police cooperation "Prüm II" which establishes a technical architecture for the exchange, the national authorities that are competent for DNA profiles,

[58]Proposal for a Regulation OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM/2021/784 final.

vehicle data, images and other police records according to the relevant proposed directive on information exchange between authorities and law enforcement of Member States to repeal the Swedish position as was done with the Framework Decision 2006/960/JHA)[59].

The Regulation has tried to amend some regulatory instruments such as the eu-LISA Regulation (2018/1726)[60], the Regulations for interoperability and information systems in the field of borders and visas (2019/817) and in the sector of police cooperation, asylum and migration (2019/818). The content of a code actually appears to have a systematic completeness linking with DNA profiles, dactyloscopic data, vehicle registration data, facial images, criminal records extracts, national contact points and, adoption of measures. A technical framework for exchanging data which is regulated primarily in Chapter 3 which provides for a central router which regulates its use for various queries and which regulates the interoperability between routers and the common identity data store for assurance purposes, traces of data processing carried out. The use of the European

[59]Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100.

[60]Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, PE/29/2018/REV/1, OJ L 295, 21.11.2018, p. 99–137.

Criminal Records Index (EPRIS) for exchange purposes are elements that require registration to processing operations.

Chapter 4 refers to “hit”, the provision for an automated exchange of basic data which limits what is necessary for the relative identification of a data subject on the extended exchange of data by carrying out the various steps for the purposes that respect mere identification.

Chapter 5 collects the provisions on access by the Member States in relation to biometric data stored by EUROPOL and originating from third countries, resulting in access by EUROPOL to data stored in the databases of the Member States.

Chapter 6 includes data relating to the purposes of the Regulation that have to do with the provisions of the related Directive (EU) 2016/680 (LED) which limits the prohibitions on the transfer of data in an automated way towards third countries or to international organizations. Supervision and audits are thus regulated to ensure and comply with the rules described.

Chapter 7 referred to the competences of the Member States, EUROPOL, and the eu-LISA dealing with the contents of the Regulation.

Chapter 8 is based on the amendments which are already referred to in the Decisions 2008/615/JHA and 2008/616/JHA and the Regulations (EU) 2018/1726, (EU) 2019/817 and (EU)

2019/818[61].

Chapter 9 has established the recognition and information obligations that carry out the notifications and the transitional provisions thus establishing the requirements for the entry into force of the establishment of a committee for the adoption of a manual for the relative implementation of the Regulation.

From justice to prevention and from the legality of criminal justice to the legality of security, a balance is sought which concerns the fragmentation of the sovereignty of the EU, the powers of sources and the scope of legality, passing to a limited concept of certainty and predictability of the law at a broad spirit of certainty as a provision in jurisprudential law.

This is a balanced security legality that foresees a technical nature between Eurounitary sources of predictability and procedural transparency as control bodies and mechanisms that give rise to dynamics of an interinstitutional conflict between EUROPOL and EDPS. We do not notice however a broad procedural transparency that guarantees the technical nature of this entire microscopic system in a dimensional way, which also reaches an even more technical and constantly evolving arrangement such as that of artificial intelligence for the coming

[61]Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11. Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 12–72.

months/years (Danaher, 2016; Burrell, 2016; Hilderbrandt, 2018; Lagioia, Sartor, 2020; Kiseleva, 2021; Tschider, 2021; Papadouli, 2022).

**References**

Adler-Nissen, R., Gammetoft Hannsen, T. (2008). *Sovereignity games. Instrumentalizing State sovereignity in Europe and beyond.* Palgrave, New York.

Bergström, M. (2011). EU anti-money laundering regulation: Multilevel cooperation of public and private Actors. In C. Eckes, T. Konstatinides. *Crime within the Area of Freedom, Security and Justice: A European Public Order.* Cambridge University Press, Cambridge, 98ss.

Bergström, M. (2018). The many uses of anti-money laundering Regulation. *German Law Journal, 19 (5),* 422ss.

Blanke, H.J., Mangiamelli, S. (2021). *Treaty on the Functioning of the European Union. A commentary.* ed. Springer, Berlin.

Brewczyńska, M. (2022). A critical reflection on the material scope of the application of the law enforcement directive and its boundaries with the general data protecting regulation. In E. Kosta, R. Leenes, I. Kamara. *Research handbook on EU data protection data.* Edward Elgar, Cheltenham.

Burrell, J. (2016). How machines think: Understanding opacity in machine-learning algorithms. *Big Data and Society, 3 (1),* 2ss.

Cassese, S. (2012). New paths for administrative law: A manifesto. *International Journal of Constitutional Law, 10 (3),* 604ss.

Chamon, M. (2016). *EU Agencies: Legal and political limits to the transformation of the EU.* Oxford University Press, Oxford.

Danaher, J. (2016). Algorithmic decision-making and the problem of opacity. *Computers and Law, 8*, 32ss.

Daskal, J. (2018). Unpacking the CLOUD act. *Eucrim, 4,* 222ss.

De Capitani, E. (2020). Progress and failure in the Area of Freedom, Security, and Justice. In F. Bignami. *EU Law in populist times: crises and prospects*. Cambridge University Press, Cambridge, 378ss.

Floridi, L. (2018). AI4people. An ethical framework for a good AI society: Opportunities, risks, principles, and reccomendations. *Minds and Machinews, 28,* 690ss.

Froehlich, A. (2022). *Spaceports in Europe.* ed. Springer, Berlin, 3ss.

Gilmore, W.C. (2004). *Dirty money: The evolution of money-laundering counter-measures.* Council of Europe Press, 3rd ed.

Goldewijk, B.K. (2008). Why human? The interlinkages between security, rights and development. *Security and Human Rights, 19 (1),* 26ss.

Henderson, K. (2005). *The Area of Freedom, Security and Justice in the enlarged Europe*. ed. Palgrave, London.

Hildebrandt, M. (2018). Algorithmic regulation and the rule of law. *Royal Society, 376,* 4ss.

Kiseleva, A. (2021, July 29). Making AI's transparency

transparent: Notes on the EU proposal for the AI. *European Law Blog*: https://europeanlawblog.eu/2021/07/29/making-ais-transparency-transparent-notes-on-the-eu-proposal-for-the-ai-act/

Lagioia, F., Sartor, G. (2020). AI systems under criminal law: A legal analysis and a regulatory perspective. *Philosophy and Technology, 33.*

Leiser, M.R., Custers, B.H.M. (2019). The law enforcement Directive: Conceptual issues of EU Directive 2016/680. *European Data Protection Law Review, 5 (3),* 370ss.

Liakopoulos, D. (2019). Regulation (EU) 2016/679 on the protection of personal data in light of the "Cambridge Analytica" affair. *E-Journal of Law. An indipendent law Journal, 5 (1)*

Luchtman M., Vervaele, J. (2014). European Agencies for criminal justice and shared enforcement (Eurojust and the European Public Prosecutor's Office). *Utrecht Law Review, 10 (5),* 134ss

Mitsilegas, V. (2022). *European Union criminal law*. Hart Publishing, Oxford, Oregon & Portland.

Mitsilegas, V., Monar J., Rees, W. (2003). *The European Union and internal security. Guardian of the people?.* ed. Palgrave, New York.

Mitsilegas, V., Mouzakiti, F. (2020). Data-driven operational

co-operation in Europe's Area of Criminal Justice. In C. Billet, A. Turmo (ed.). *Coopération opérationnelle en droit pénal de l'Union européenne.* ed. Brulyant, Bruxelles, 132

Nunzi, A. (2007). Exchange of information and intelligence among law enforcement authorities a European Union perspective. *Revue International de Droit Pénal, 78 (1-2)*, 149ss.

Pagallo, U., Quattrocolo, S. (2018). The impact of AI on criminal law, and its twofold aspects. In W. Barfield, U. Pagallo, (ed.). *Research handbook on the law of artificial intelligence*. ed. Elgar Publisher, Cheltenham, 393ss.

Papadouli, V. (2022). Transparency in artificial intelligence: A legal perspective. *Journal of Ethics and Legal Technologies, 4 (1),* 27ss.

Quintel, T. (2022). Data protection rules applicable to Financial Intelligence Units: Still no clarity in sight. *ERA Forum, 23,* 57ss.

Sicurella, R., Scalia, V. (2013). Data mining and profiling in the Area of Freedom, Security and Justice: State of play and new challenges in the balance between security and fundamental rights protection. *New Journal of European Criminal Law, 4 (3),* 410ss.

Slobogin, C. (2018). Preventive justice: A paradigm in need of testing. *Behavioral Sciences and the Law, 36 (4)*, 5ss.

Tschider, C.A. (2021). Legal opacity: Artificial Intelligence's

sticky wicket. *Iowa Law Review Online, 106,* 128ss.

Wood, M. (2018). Mapping EU Agencies as political entrepreneurs. *European Journal of Political Research, 57 (2),* 406ss.